

66/02/60

**UTILITY PATENT APPLICATION TRANSMITTAL**  
**(Large Entity)***(Only for new nonprovisional applications under 37 CFR 1.53(b))*Docket No.  
12640 (GE998-072)

Total Pages in this Submission

**TO THE ASSISTANT COMMISSIONER FOR PATENTS**Box Patent Application  
Washington, D.C. 20231

Transmitted herewith for filing under 35 U.S.C. 111(a) and 37 C.F.R. 1.53(b) is a new utility patent application for an invention entitled:

**METHOD AND SYSTEM FOR SECURELY HANDLING INFORMATION BETWEEN TWO  
INFORMATION PROCESSING DEVICES**

and invented by:

Uwe Hansmann  
Frank SeligerJc675 U.S. PTO  
09/398876  
09/20/99If a **CONTINUATION APPLICATION**, check appropriate box and supply the requisite information:☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: \_\_\_\_\_

Which is a:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: \_\_\_\_\_

Which is a:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: \_\_\_\_\_

Enclosed are:

**Application Elements**

1. ☒ Filing fee as calculated and transmitted as described below
2. ☒ Specification having 35 pages and including the following:
  - a. ☒ Descriptive Title of the Invention
  - b. ☐ Cross References to Related Applications *(if applicable)*
  - c. ☐ Statement Regarding Federally-sponsored Research/Development *(if applicable)*
  - d. ☐ Reference to Microfiche Appendix *(if applicable)*
  - e. ☒ Background of the Invention
  - f. ☒ Brief Summary of the Invention
  - g. ☒ Brief Description of the Drawings *(if drawings filed)*
  - h. ☒ Detailed Description
  - i. ☒ Claim(s) as Classified Below
  - j. ☒ Abstract of the Disclosure

**UTILITY PATENT APPLICATION TRANSMITTAL**  
**(Large Entity)**

*(Only for new nonprovisional applications under 37 CFR 1.53(b))*

Docket No.  
12640 (GE998-072)

Total Pages in this Submission

**Application Elements (Continued)**

3. ☒ Drawing(s) *(when necessary as prescribed by 35 USC 113)*
- a. ☒ Formal                      Number of Sheets 3
- b. ☐ Informal                      Number of Sheets \_\_\_\_\_
4. ☒ Oath or Declaration
- a. ☒ Newly executed *(original or copy)*                      ☐ Unexecuted
- b. ☐ Copy from a prior application (37 CFR 1.63(d)) *(for continuation/divisional application only)*
- c. ☒ With Power of Attorney                      ☐ Without Power of Attorney
- d. ☐ DELETION OF INVENTOR(S)  
Signed statement attached deleting inventor(s) named in the prior application,  
see 37 C.F.R. 1.63(d)(2) and 1.33(b).
5. ☐ Incorporation By Reference *(usable if Box 4b is checked)*  
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied  
under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby  
incorporated by reference therein.
6. ☐ Computer Program in Microfiche *(Appendix)*
7. ☐ Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all must be included)*
- a. ☐ Paper Copy
- b. ☐ Computer Readable Copy *(identical to computer copy)*
- c. ☐ Statement Verifying Identical Paper and Computer Readable Copy

**Accompanying Application Parts**

8. ☒ Assignment Papers *(cover sheet & document(s))*
9. ☐ 37 CFR 3.73(B) Statement *(when there is an assignee)*
10. ☐ English Translation Document *(if applicable)*
11. ☐ Information Disclosure Statement/PTO-1449                      ☐ Copies of IDS Citations
12. ☐ Preliminary Amendment
13. ☒ Acknowledgment postcard
14. ☒ Certificate of Mailing
- ☐ First Class                      ☒ Express Mail *(Specify Label No.):* EM580751319US

**UTILITY PATENT APPLICATION TRANSMITTAL**  
**(Large Entity)**

*(Only for new nonprovisional applications under 37 CFR 1.53(b))*

Docket No.  
12640 (GE998-072)

Total Pages in this Submission

**Accompanying Application Parts (Continued)**

15. ☒ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*

16. ☒ Additional Enclosures *(please identify below):*

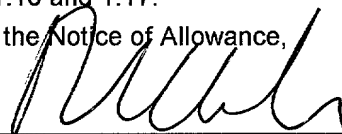
Associate Power of Attorney and Request for Change of Mailing Address

**Fee Calculation and Transmittal**

**CLAIMS AS FILED**

For	#Filed	#Allowed	#Extra	Rate	Fee
Total Claims	40	- 20 =	20	x \$18.00	\$360.00
Indep. Claims	4	- 3 =	1	x \$78.00	\$78.00
Multiple Dependent Claims (check if applicable) <input type="checkbox"/>					\$0.00
BASIC FEE					\$760.00
OTHER FEE (specify purpose) Assignment recordal fee					\$40.00
TOTAL FILING FEE					\$1,238.00

- ☐ A check in the amount of \_\_\_\_\_ to cover the filing fee is enclosed.
- ☒ The Commissioner is hereby authorized to charge and credit Deposit Account No. 50-0510/IBM as described below. A duplicate copy of this sheet is enclosed.
- ☒ Charge the amount of \$1,238.00 as filing fee.
- ☒ Credit any overpayment.
- ☒ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
- ☐ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).



Signature

**Richard L. Catania**  
Registration No. 32,608  
**SCULLY, SCOTT, MURPHY & PRESSER**  
400 Garden City Plaza  
Garden City, NY 11530  
(516) 742-4343

Dated: September 20, 1999

CC:

**CERTIFICATE OF MAILING BY "EXPRESS MAIL" (37 CFR 1.10)**Applicant(s): **Uwe Hansmann, et al.**

Docket No.

**12640 (GE998-072)**

Serial No.

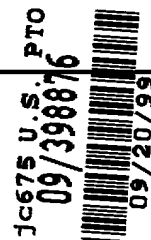
**unassigned**

Filing Date

**herewith**

Examiner

Group Art Unit

**unassigned**Invention: **METHOD AND SYSTEM FOR SECURELY HANDLING INFORMATION BETWEEN TWO INFORMATION PROCESSING DEVICES**I hereby certify that this **New Patent Application***(Identify type of correspondence)*

is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 in an envelope addressed to: The Assistant Commissioner for Patents, Washington, D.C. 20231

on **September 20, 1999***(Date)***Mishelle Spina***(Typed or Printed Name of Person Mailing Correspondence)**(Signature of Person Mailing Correspondence)***EM580751319US***("Express Mail" Mailing Label Number)***Note: Each paper must have its own certificate of mailing.**

METHOD AND SYSTEM FOR SECURELY HANDLING  
INFORMATION BETWEEN TWO INFORMATION PROCESSING DEVICES

BACKGROUND OF THE INVENTION

5

Technical Field

The present invention generally relates to secure  
interoperation between two information processing devices  
where only one of these devices can handle information in  
a secure manner. In particular, the present invention  
relates to a method and a system for securely handling an  
information unit by a first information processing  
device, for instance a terminal device, interoperating  
with a second secure information processing device, for  
instance a portable device like a chip card, whereby the  
information unit is provided by an issuer.

10

15

Prior Art

It is commonly known that chip cards are not only  
utilized as a memory for storing data on it but also used  
as an access control medium or a medium to enable and  
perform encryption and decryption of information.  
Therefore, from the beginning of development of chip  
cards, the field of cryptology has played a central or  
even dominant role. Meanwhile, the scientific results of  
this development field are inseparably related to chip  
card technology.

20

25

The technical field of cryptology divides into two fields  
of activity, namely cryptography and cryptoanalysis, The  
field of cryptography embraces the science and  
methodology of encryption and decryption of information.

30

The science of cryptanalysis addresses to crack existing cryptographic systems.

5 In the field of chip card technology, another major issue is practicability of the scientific and theoretical aspects of cryptology.

10. The predominant objective of cryptology is, on the one hand, secrecy of information and, on the other hand, securing or safeguarding the authentication of information. Both objectives are independently of each other and thus have different requirements of the respective information system. 'Secrecy' means that only the addressed receiver is able to decrypt the contents of a message. In contrast to that, 'authenticity' enables the receiver of the message to secure that the received message has not been altered during transmission.

15  
20 For the following description of known techniques of data encryption/decryption it is referred to chapter 4 of the "Handbuch der Chipkarten", W. Rankl, W. Effing, 1996, Hauser Verlag, Munich-Vienna, which contents are regarded to be fully incorporated herein. Each encryption technique uses three types of information. Non-encrypted data are designated as "plain text" wherein encrypted data are designated as "cypher text". For encryption/decryption one or more keys are required as third type of data. All these types of data are to be processed by an encryption algorithm. Cryptographic algorithms currently used in chip cards are generally  
25  
30 block-oriented, which means that the plain text and the cypher text are always processed as packages of a given

length, e.g. 8 byte in case of the algorithm used by the decryption/encryption standard (DES) which is discussed in more detail in the following.

5 It is emphasized hereby that the present invention is applicable to all described fields of cryptography like encryption, decryption, or one-way cryptographic functions like hash values or digital signature verification mechanism. Modern cryptographic algorithms  
10. are generally based on the known Kerckhoff principle which says that the entire security of an algorithm shall only depend on secrecy of the underlying keys, but not on secrecy of the cryptography algorithm itself.

15 Besides Kerckhoff, a further known principle is security through masking which presumes that a fictitious attacker does not know how the system works. But the latter principle is by no means sufficient to secure an information handling system. The security of modern and  
20 already published cryptographic algorithms does, in practice, only depend on the performance of the computers used to crack a cryptographic algorithm and thus an alleged additional masking technique of the utilized methodology of crypton one achieves a considerably  
25 increased protection against attacks. Otherwise, the rapidly progressing development of computer performance causes a doubling of performance within about one and a half years and thereupon the increasing number of participants of the worldwide computer network, e.g. the  
30 WEB, provide a further way to perform serious attacks on cryptographic systems or related keys.

In order to crack a cryptographic algorithm, there are different ways of attacks. A first one is the "cypher text only attack" where the attacker does only know the cypher text and tries to obtain the key or plain text by use of this information. A more promising attack is the so-called "known plain text attack" where the attacker is in the possession of a number of plain-text/cypher-text pairs for a secret key. The secret key can be obtained by trial and error. The most trivial attack is to find out the secret key only through trial and error which is called "brute force attack". By using a large performance computer, on the basis of a known plain-text/cypher-text pair, all feasible encryption keys are tried until the right one is obtained. The teaching of statistics says that on an average only the half of all possible keys has to be checked in order to find the right one. For that reason, a large space of possible keys renders that kind of attack more difficult.

Cryptographic algorithms are further divided into symmetric and asymmetric algorithms, dependent on the respectively utilized key. 'Symmetric' means that algorithm for en- and decryption is using the same key. In contrast to that, 'asymmetric' cryptographic algorithms, like that proposed by Whitfield Diffie and Martin E. Hellman in 1976, are using different keys for encryption and decryption. The two major principles for a well performing encryption algorithm are the principles of 'confusion' and 'diffusion' after C. Shannon. It is emphasized that both types of algorithms can be taken as a basis for the present invention.



Symmetric cryptographic algorithms are based on the principle of utilizing the same key for both encryption and decryption. A well-known data encryption algorithm called 'Data Encryption Algorithm' (DEA) has been proposed by the applicant of the present application together with the U.S. National Bureau of Standards developed in 1977. This standard algorithm is often be referred to as 'Data Encryption Standard' (DES). Since that algorithm is designed in consideration of Kerckhoff's dogma, it could be published without any impact on its security. For the details of that algorithm it is further referred to National Institute of Standards and Technology (NIST), FIPS Publication 46-2, "Data Encryption Standard", December 1993.

The principle of 'confusion' means that the statistics of the cypher text shall influence the statistics of the plain text so that an attacker can not take profit by that. The second principle "diffusion" means that every bit of the plain text and of the key shall influence as much bits of the cypher text as possible.

The DEA is a symmetric encryption algorithm using block architecture. It does not perform expansion of the cypher text which means that plain text and cypher text are of identical length. The block length is 64 bit (=8 byte), the key is also 64 bit long but includes 8 parity bits whereby the available space of possible keys is considerably reduced which is in case of DES  $2^{56} = 7.2 \times 10^{16}$  possible keys. But in view of the continuously and permanently increasing computer performance such a space

of possible keys is regarded as the lower limit for the required security of a cryptographic algorithm.

As an exemplary asymmetric cryptographic algorithm, it is referred to the one proposed by Whitfield Diffie and Martin E. Hellman, published in 1976, which is based on two different keys. One of these keys is public, the other is secret. An information or message is encrypted by using the public key prior to transmission of an information and only the owner of the secret key is enabled to decrypt again the encrypted message. In particular, that principle for the first time enables implementation of a digital signature which in principle can be verified by everyone who is in the possession of the required (public) key. Exemplarily, it is referred to a first implementation of the prementioned principle for asymmetric cryptographic algorithms, namely the 'RSA' algorithm proposed by Ronald L. Rivest, Adi Shamir and Leonard Adleman which is the currently best known and most versatile asymmetric cryptographic algorithm. Its functional principle is based on the arithmetic of big integer numbers. Both keys are generated based on two big prime numbers. Encryption and decryption can be mathematically expressed by a modulo function, namely in case of encryption  $y = x^e \bmod n$ , for decryption  $x = y^d \bmod n$  with  $n = p \times q$  wherein  $x$  = plain text,  $y$  = cypher text,  $e$  = public key,  $d$  = secret key,  $n$  = public modulus and  $p$ ,  $q$  = secret prime numbers.

For the further details of an implementation of the RSA algorithm it is accordingly referred to R.L. Rivest, A. Shamir, and L.M. Adleman "A Method for obtaining Digital

Signatures and Public-Key Cryptosystems", Communications of the ACM, 21(2), pages 120-126, February 1978.

5 In addition to secrecy of information, another paradigma  
for encryption algorithms is 'authenticity' of a received  
message of information. As mentioned above, authenticity  
means that a message is not altered e.g. not manipulated.  
For that purpose, to the actual message a message  
10 authentication code is appended and both parts are  
transmitted to the receiver. The receiver is enabled to  
calculate its own message authentication code (MAC) and  
compares that code with the received code. In case of  
both matching, it is secured that the transmitted message  
has not been altered during transmission. For generating  
15 a MAC, a cryptographic algorithm with one secret key  
which is known to both communication partners is  
utilized. For the calculation of a MAC in principle  
every cryptographic algorithm can be used, but in  
practice, the above mentioned DEA algorithm is utilized  
20 nearly exclusively.

A particular scenario for the present invention is a  
situation where a chip card is inserted in a chip card  
acceptance device - in the following called "terminal  
25 device" - which does not yet have a support module  
capable of accessing the card or to fulfill a particular  
function of the chip card on the terminal. Therefore it  
is required to obtain the missing software component from  
an other source of information e.g. to download such  
30 required module from a central server connected to the  
internet. It is noted that the terminal device can  
either be a computer, like a personal computer or network

computer with a chip card reader/writer hardware, or a specialized device combining the chip card reader/writer hardware with an embedded computer.

5 The transmission will often take place over a network that is open to attacks. It is known that the chip card hereby ensures that the software component in the device accessing the chip card shares a secret to the chip card by using mechanisms called external authentication or  
10 challenge/response. Further, it is known that a digital signature secures the download of software but the public keys of all potential senders have to be stored on the hard disk of the computer. Therefore, it is necessary that it can be ensured that the software was not altered  
15 on its way through the network and that the software was sent by the owner of the public key. But getting the public key for signature verification must also be done in a secure way, before the download is secure. This requires a chain of certification authorities.

20 On the other hand, an authentication mechanism is needed to verify that the obtained software component is the most recent issued release of that software. Today, the version control is handled by continuously increasing a  
25 version number.

#### SUMMARY OF THE INVENTION

It is therefore an object of the present invention to provide a method and a system for securely interoperating  
30 a first information processing device, in particular a terminal device like a chip card reader, and a second secure information processing device, in particular a

portable device like a chip card, where the first device does not yet have an information unit like a software component required for interoperating the first and the second device like providing or controlling access to the second secure device. It is therefore required that the missing information unit is obtained from an other source of information. A particular object of the invention which is strongly related to the above object is that gathering the missing information unit is to be accomplished in a secure manner.

In order to solve the above objects and to avoid the above-mentioned drawbacks of existing mechanisms and systems, the invention proposes that the information unit is provided from the issuer to the first information processing device whereby the information unit is processed by a cryptographic process i.e. for instance encrypted and/or signed by a signature. The required key for the cryptographic process is particularly provided on the second secure information processing device. The information unit is cryptographically reprocessed i.e. for example decrypted and/or its signature verified by using the key. It is emphasized that the information unit can be secured by alternatively using encryption/decryption and signature verification or by using both mechanisms in parallel.

#### BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the present invention will now be described, by way of example only, with reference to the accompanying drawings in which:

Fig. 1 a schematic view of a preferred embodiment of the invention together with the underlying data flow;

Fig. 2a a flow diagram illustrating a method for encryption/decryption according to the invention;

Fig. 2b a flow diagram according to Fig. 2a in a case of a signing/signature verification.

#### DETAILED DESCRIPTION OF THE INVENTION

According to a first preferred embodiment, the information unit is provided from the issuer to the first information processing device whereby the information unit is encrypted by using a first key which is also provided in an encrypted format by using a second key. The second key is provided on the second secure information processing device and interconnecting the first information processing device and the second secure information processing device therefore enables to decrypt the first key by using the second key. By using the decrypted first key, the information unit can also be decrypted.

According to a second preferred embodiment of the invention, the information unit is provided from the issuer to the first information processing device whereby the information unit is signed by using a signature. The signature is provided from the issuer to the first information processing device whereby the signature is generated by using at least one key. Further the at least one key for signature verification is provided on the second secure information processing device. After

the first information processing device and the second secure information processing device have been interconnected, the at least one key for signature verification is transferred from the second secure information processing device to the first information processing device. Finally the signature of the information unit is verified by using the at least one key.

10. It is noteworthy that the information unit can be any set of (pure) data or an executable code like an application program or a hardware driver to run on the second secure device and/or the other device(s), i.e. any kind of information. Further the information unit can serve to run specific functions of the second secure device on the first device or on at least a third device attached to the first device. In particular, the information unit can provide an access control for the second secure device. Further, the second secure information processing device can be any device where the issuer of that device, and of the information unit, can secure that the private key "i" is secure and not alterable, i.e. securely stored on the device. Exemplary devices are chip cards, in particular smart cards, Personal Computers with an according access control, or any other portable devices like laptops, palmtops, organizers, etc. Accordingly, the first information processing device can be any device with which the second secure device can interoperate like a card accepting device, e.g. a card reader, or even a computer with a card accepting device attached thereto.

In particular, according to the invention, the second secure device provides the second key by which the first key has been encrypted and therefore interconnecting the first device and the second device enables firstly to  
5 decrypt the first key by using the second key and, secondly, to decrypt the information unit by using the decrypted first key. The basic concept of the invention therefore is to have the private (second) key securely stored on the second secure information processing device  
10 what guarantees that this key will remain private i.e., can not be gathered by a third party.

In case of a chip card and a chip card accepting device, the invention particularly enables dynamic secure  
15 download and execution of a missing software support, for instance support needed for specific functions of a chip card on a device attached to the chip card acceptance device. The software component can only be decrypted by the usage of a key "T". This key is transmitted in an encrypted form as key " $T_i$ " together with the software encrypted with it. Key " $T_i$ " can only be decrypted by the  
20 chip card knowing the key "I" that was used to encrypt the key "T". The key "I" is stored on the chip card by the issuer at the time of card issuing. One of the advantages of this procedure is that the issuer of the  
25 card can secure that the key "I" is a private key insofar as it is guaranteed that the key is not known by others. Further, any laterly required software support for the chip card can be secured by using this key. On the other  
30 hand, the session key "T" which maybe will be known by others through transfer to the terminal device, can be changed by the issuer from session to session thus



considerably enhancing data security. To make the card decrypt key " $T_i$ " using key "I", a command (APDU) is passed to the chip card that was transmitted together with the software module to be decrypted and used. In other words, the chip card which may be controlled by the downloaded software, itself plays a critical role in securing the integrity of the driving software. Insofar, the chip card itself retrieves the key T which has been used to encrypt the downloaded software via decryption of the encrypted key  $T_i$ . To prevent alteration of the transmitted software module, it is proposed that it will be encrypted or signed with one of the standard algorithms described in the introductory part. The issuer of the software has the required encryption, decryption or signature keys. Instead of requiring the terminal device to store and retrieve the matching decryption key or fetch the matching certificate, the present invention describes a way of using the chip card itself to retrieve that key. The chip card advantageously is the most secure and most convenient way to store the secret decryption key or the certificate or the card issuer. In this way, only software that is certified by the card issuer should be allowed to access the card.

It is emphasized that beyond encryption/decryption the invention can also employ digital signing or digital signature verification for the encryption by using the first key and/or the second key. For this signature case, the described mechanism provides a trusted way to the issuer's public signature key without the requiring complex certificate handling including chains of trust.

5 The information unit can advantageously be a program  
module or data to control access to a portable device by  
the terminal device, the integrity of the information  
unit hereby playing a rather critical role for data  
security. Further, the information unit can be an  
application program which can run either on the portable  
device or the terminal device or can serve to run  
specific functions of the portable device on the terminal  
device or on a second device attached to the terminal  
10 device. Also in these cases, data integrity plays a  
dominant role.

15 Portable devices like chip cards commonly provide only  
limited resources for processing data and according  
limited space for storing data. Therefore, according to  
another embodiment of the invention, both the decryption  
of the first key and the decryption of the information  
unit are accomplished on the terminal device's side.

20 In order to provide a more powerful and automatically  
operating system, according to another embodiment of the  
invention the first device provides a control command  
(APDU) to the second secure device which initiates or  
triggers the transfer of the second key to the first  
25 device, or initiates or triggers the beginning of  
decryption of the first key by using the second key.  
Hereby an operating system or program of the first device  
advantageously must not know how to decrypt key "T<sub>1</sub>" and  
can be freed from performing the decryption procedure.  
30 The first device only passes the APDU command to the  
second secure device. This embodiment enables that the  
entire procedure proposed by the invention can be

performed in the background i. e. not visible to the user whereby in particular the required second key is transferred to the first device without any needed interaction by the user.

5

In a preferred embodiment of the invention, the encrypted information unit and the encrypted first key are downloaded from a central server, e.g. a server interconnected with the Internet, particularly from a server provided by the issuer of the second secure device. Alternatively, the above mentioned control command can be downloaded, too, from such a server. In view of the continuously increasing meaning of the Internet, such kind of software support via download is a preferred way to obtain a required information unit.

10-  
15

In a further preferred embodiment of the invention, the second key required to decrypt the first key is securely stored on the second secure device at time of its issuing by the issuer. Since the issuer of the card will often be identical with the issuer of the information unit, it is hereby guaranteed that the second key will be compatible with the encryption of the first key.

20

According to a further embodiment of the invention, a third key can be used for authentication or version control of the underlying information unit. Hereby the second secure device contains a version number and a key "E" which the downloaded information unit accessing the second secure device must know. To prove that the information unit has the matching key "E", a challenge/response mechanism ("external authentication")

25  
30

is used. This allows the issuer of the second secure device by changing the key "E" on that device, in combination with the other steps of the proposed mechanism, to initiate the second secure device and/or the first device to download a new version of the underlying information unit.

Using such a third key, it is possible to realize a further automatization of the proposed mechanism where the first device is initiated to download a new release of the information unit.

The proposed arrangement of the two different key levels enables, in accordance with another preferred embodiment of the invention, that the first key can be randomized between different sessions of interoperating the first and the second device, i. e. the issuer of the second secure device every time can use another random key T to encrypt the information unit with the cryptographic function. Therefore, it is advantageously not compromising the security that the key T is given back from the second device to the first device in a clear form.

It is emphasized again that the method and system according to the invention can be applied to signing and signature verification accordingly.

Further features, details and advantages of the present invention will become evident from the following detailed description of embodiments of the invention and the corresponding accompanying drawings,

Fig. 1 depicts a scenario where a chip card 1 is inserted in a chip card reader 2 which does not yet have a required software component capable of accessing the chip card 1. Therefore the operating system of the card reader 2 initiates that the missing software component be downloaded 3 from a central server 4 to the card reader 2. In order to validate that the downloaded software component was certified by the issuer and has not been altered in the meantime, in accordance with the invention, the following mechanism is proposed. The issuer's certificate and corresponding private key "I" is stored on the chip card 2 at the time the card is issued. Prior to the software download 3, an encryption with a session key "T" is applied to the underlying software component. The downloaded data therefore contains the cyphered software plus key "T<sub>i</sub>", i. e. the key "T" encrypted by a key "I", plus a command (APDU) to trigger or to make the chip card 1 decrypt key "T<sub>i</sub>". The APDU command, when sent to the chip card 1, results in a decryption of the key "T<sub>i</sub>" to reveal key "T" that was used to encrypt the software component. Due to the above-mentioned combination of two different key levels, the card issuer can every time change key "T" by another random key to encrypt the service with the cryptographic function. Therefore, it is not compromising the security that the key "T" is given back from the chip card 1 to the card reader 2 (terminal device) in clear form. The software module, in this embodiment, is to drive the terminal device 2 to access the chip card 1, but such a software module can also be an application program to run on either the chip card 1 or the terminal device 2 or fulfill specific functions on

the terminal device 2 or another (optional) device 5  
connected or attached to the terminal device 2. The  
device 5 can be part of the terminal device and can be  
any information handling device or system, or only part  
of such a system like a video display or the like.  
Normally the terminal device 2 will be a non-intelligent  
card accepting device and the device 5 an intelligent  
card reader. Further, the software module can be a driver  
to drive the chip card or an instrument to control access  
to the chip card itself.

It is emphasized that the functionality of the terminal  
device as proposed by the invention can be implemented by  
means of common memory and processor hard- and software  
components.

The underlying encryption/decryption process consists of  
the following steps. The information unit  $s$  is encrypted  
by using the key "T" and the key "T" is encrypted by  
using key "I" as follows:

$$\begin{aligned}x &= \text{enc}(s, T); \\ T_i &= \text{enc}(T, I).\end{aligned}$$

Both " $x$ " and " $T_i$ " are transferred from the central server  
4 to the card reader 2. The card reader 2 then instructs  
the chip card 1 to decrypt " $T_i$ " using "I":

$$T = \text{dec}(T_i, I).$$



(support module +  $T_i$  + APDU) can be downloaded as one file, e. g. in a compressed format using known compression tools like "WINZIP" or "PKZIP".

5 Then the 'APDU' control command is sent 26 to the chip card in order to initiate or to trigger the chip card to decrypt 27 the encrypted key " $T_i$ " by using key "I". Alternatively the chip card can be initiated to transmit the key "I" to the card reader and the decryption of " $T_i$ " performed by the card reader. In case the chip card fulfills the decryption, the decrypted key "T" will be transferred back 28 to the card reader and then the support module be decrypted 29 by an operating system or program available on the card reader, by using the key 10- "T". The resulting decrypted support module then will be 15 executed 23 by the card reader.

In case of an underlying signature/signature verification, the mechanism proposed by the invention 20 consists of the following steps. The information unit "s" is signed by using a signature key "I":

$$x = \text{sign}(s, I_{\text{priv}}).$$

25 Both "x" and "s" are transferred from the central server 4 to the card reader 2. The card reader 2 then gathers the key "I" for signature verification from the chip card 1 and performs the following signature verification operation:

30  $\text{signver}(s, x, I_{\text{pub}}) == \text{OK} ?$



5 A corresponding flow diagram depicted in Fig. 2b shows  
the proposed mechanism in case of the signing/signature  
verification instead of the above described data  
encryption/decryption. As in Fig. 2a, after the chip card  
is inserted 30 in the card reader, the card reader checks  
whether a required support module is locally available  
31. If so 32, the module is executed 33. If not 34, the  
required module and the 'APDU' command are downloaded 35  
from the central server whereby the module is signed with  
10- a private key " $I_{priv}$ ". The 'APDU' command is accordingly  
sent 36 to the chip card in order to initiate or trigger  
the chip card to send back 37 a public key " $I_{pub}$ " which is  
necessary to verify 38 the signature. According to the  
teaching of the invention, the required public key " $I_{pub}$ "  
15 is provided by the chip card itself and transferred to  
the terminal device at first when having received the  
'APDU' command. This key is then used to verify the  
signature of the downloaded module and in case of a  
matching signature 39, the software module is executed  
20 33, for instance in order to drive the chip card to  
execute a particular application either in the chip card  
or the card reader. If both signatures do not match 40,  
an error message of the kind 'Invalid Signature' is  
output by the card reader, e. g. acoustically or by means  
25 of a display.

In cases where the card reader has a secure software  
execution that only allows code to be executed that was  
validated by the chip card, i. e. it can not only be  
30 ensured that the downloaded software was not altered, but  
also that the software was certified by the issuer of the

card, and that the version of the software is appropriate.

5 Thereupon it is secured that the code can only be executed if it was certified by the issuer of the card, the issuer can make sure that the software accessing the card does not make any operations that can insecure the system like sending data to somebody else or logging data.

10 For a version control, the following step can be added to the sequence of steps depicted in either Fig. 2a or Fig. 2b:

15 External authentication with key "E" in order to verify that the version of the software module matches the smart card.

20 Authentication is herein regarded as any process through which one proves and verifies certain information. A chip card commonly uses external authentication to establish the identity of the terminal. This is done by ensuring that the terminal device shares a secret with the chip card.

25 An external authentication starts with the chip card wondering about the terminal's identity and sending a challenge - for example a random 8-byte sequence - to the terminal whose identity is being questioned. The terminal  
30 receiving the challenge encrypts it with its secret, a particular key, and sends back the encrypted result. The chip card now decrypts the encrypted message using the

key it knows the terminal possesses if it is authentic.  
If the message decrypts satisfactorily, i. e. the  
decrypted challenge is identical to the challenge  
originally sent by the chip card, then the chip card  
5 knows that the terminal possesses a particular key and  
this establishes its identity.

While the invention has been particularly shown and  
described with respect to preferred embodiments thereof,  
10. it will be understood by those skilled in the art that  
the foregoing and other changes in form and details may  
be made therein without departing from the spirit and  
scope of the invention.

### CLAIMS

Having thus described our invention, what we claim as new, and desire to secure by Letters Patent is:

1           1.           A method for securely handling an information  
2                   unit by a first information processing device  
3                   (2) interoperating with a second secure  
4                   information processing device (1), in  
5                   particular a chip card, whereby the information  
6                   unit is provided by an issuer,

7  
8                   the method comprising the steps:

9                   providing (3, 25, 35) the information unit from  
10                   the issuer to the first information processing  
11                   device (2), the information unit being  
12                   processed by a cryptographic process;

13  
14                   providing at least one key for the  
15                   cryptographic process on the second secure  
16                   information processing device (1); and

17  
18                   cryptographically reprocessing (29, 38) the  
19                   information unit by using the at least one key.

1           2.           The method according to claim 1, comprising:

2                   providing (3, 25, 35) the information unit from  
3                   the issuer to the first information processing  
4                   device (2), the information unit being  
5                   encrypted by using at least a first key;

6 providing the first key from the issuer to the  
7 first information processing device (2), the  
8 first key being encrypted by using at least a  
9 second key;

10  
11 providing the at least one second key on the  
12 second secure information processing device  
13 (1);

14  
15- interconnecting the first information  
16 processing device (2) and the second secure  
17 information processing device (1);

18 on side of the second secure information  
19 processing device, decrypting (27) the at least  
20 first key by using the at least second key; and

21  
22 decrypting (29) the information unit by using  
23 the decrypted at least first key.

1 3. The method according to claim 1, comprising:

2 providing (3, 25, 35) the information unit from  
3 the issuer to the first information processing  
4 device (2), the information unit being signed  
5 by using a signature;

6 providing the signature from the issuer to the  
7 first information processing device (2), the  
8 signature being generated by using at least one  
9 key;  
10

11 providing the at least one key for signature  
12 verification on the second secure information  
13 processing device (1);  
14  
15 interconnecting the first information  
16 processing device (2) and the second secure  
17 information processing device (1);  
  
18 transferring the at least one key for signature  
19 verification from the second secure information  
20 processing device to the first information  
21 processing device; and  
22  
23 verifying the signature of the information unit  
24 by using the at least one key.

1 4. The method according to claim 2, wherein the  
2 decrypted at least first key is transferred to  
3 the first information processing device (2) and  
4 the information unit is decrypted (29) on side  
5 of the first device (2).

1 5. The method according to claim 1, wherein the  
2 first information processing device (2)  
3 provides a control command (26, 36) to the  
4 second secure information processing device (1)  
5 to initiate decryption of the at least first  
6 key by using the at least second key and/or to  
7 initiate transferring the signature key for  
8 signature verification from the second secure  
9 device to the first device.

1 6. The method according to claim 5, wherein the  
2 encrypted information unit, the encrypted first  
3 key, and/or the signature key, and/or the  
4 generated signature, and/or the control command  
5 are downloaded (25, 35) from a central server  
6 (4).

1 7. The method according to claim 3, wherein the  
2 second key and/or the key for signature  
3 verification are/is securely stored on the  
4 second secure device (1) at time of its issuing  
5 by the issuer.

1 8. The method according to claim 2, wherein at  
2 least a third key is provided for external  
3 authentication and/or release control of the  
4 respective information unit.

1 9. The method according to claim 8, wherein the  
2 first device (2) is initiated to gather a new  
3 release of the information unit from the  
4 issuer, depending on the respective status of  
5 the third key.

1 10. The method according to claim 9, wherein the  
2 new release of the information unit is  
3 downloaded from an internet server (4) provided  
4 by the issuer.

1 11. The method according to claim 2, wherein the at  
2 least first key and/or the signature are/is  
3 randomized between different sessions of

4 providing the information unit from the issuer  
5 to the first device (2).

1 12. The method according to claim 1, wherein the  
2 first information processing device (2) is a  
3 terminal device, and the second secure  
4 information processing device (1) is a portable  
5 device.

1- 13. The method according to claim 12, wherein the  
2 terminal device is a chip card reader and the  
3 portable device is a chip card.

1 14. A system for securely handling an information  
2 unit, comprising a first information processing  
3 device (2) interoperating with a second secure  
4 information processing device (1), in  
5 particular a chip card, the information unit  
6 being provided by an issuer,

7 comprising:

8 the first device (2) comprising  
9 a storage for storing the information  
10 unit; and

11  
12 the second secure device (1) comprising  
13 a storage (6) for storing at least one key  
14 for a cryptographic process; and



15 providing means for cryptographically  
16 reprocessing the information unit by using the  
17 at least one key.

1 15. The system according to claim 14, wherein  
2 the first device (2) comprises  
3 a storage for storing the information  
4 unit, encrypted by using at least a first  
5 key, and a storage for storing the first  
6 key, encrypted by using at least a second  
7 key;  
8 the second secure device (1) comprises  
9 a storage (6) for storing the at least one  
10 second key, and processing means for  
11 decrypting the at least first key by using  
12 the at least second key; and  
13 providing means for decrypting the information  
14 unit by using the decrypted at least first key.

1 16. The system according to claim 14, wherein  
2  
3 the first device (2) comprises  
4 a storage for storing the information unit  
5 and a signature for the information unit;  
6 the second secure device (1) comprises  
7 a storage (6) for storing at least one  
8 signature key;

9 providing means for verifying the signature of  
10 the information unit by using the at least one  
11 signature key.

1 17. The system according to claim 14, wherein the  
2 second secure device (1) provides an access  
3 control by means of the information unit.

1 18. The system according to claim 14, wherein the  
2 second secure device (1) comprises a processor  
3 to make specific functions of the second secure  
4 device usable/accessible on the first device or  
5 on at least a third device (5) attached to the  
6 first device.

1 19. The system according to claim 14, wherein the  
2 first device (2) comprises processing means for  
3 decrypting (29) the information unit by use of  
4 the decrypted at least first key.

1 20. The system according to claim 14, wherein the  
2 second secure device (1) comprises means to  
3 initiate decryption of the at least first key  
4 by using the at least second key and/or means  
5 to initiate transfer of the signature key for  
6 signature verification from the second secure  
7 device to the first device.

1 21. The system according to claim 14, wherein the  
2 first device (2) comprises means to download  
3 the encrypted information unit, the encrypted  
4 first key, and/or the generated signature,

5 and/or the control command, from a central  
6 server (4).

1 22. The system according to claim 14, wherein the  
2 second secure device (1) comprises a non-  
3 erasable storage to store the second key and/or  
4 the signature key at time of its issuing.

1 23. The system according to claim 14, wherein the  
2 first device (2) and/or the second secure  
3 device (1) comprise/s a storage (6) for storing  
4 at least a third key for external  
5 authentication and/or release control of the  
6 information unit and processing means (7) for  
7 processing the third key.

1 24. The system according to claim 23, wherein the  
2 first device (2) comprises means to initiate  
3 download of a new release of the information  
4 unit, depending on the respective status of the  
5 third key.

1 25. The system according to claim 21, wherein the  
2 central server (4) comprises a randomizer for  
3 randomizing the at least first key and/or the  
4 signature between different sessions of  
5 providing the information unit from the issuer  
6 to the first device.

1 26. The system according to claim 14, wherein the  
2 first information processing device (2) is a  
3 terminal device, and the second secure

4 information processing device (1) is a portable  
5 device.

1 27. The system according to claim 26, wherein the  
2 terminal device is a chip card reader and the  
3 portable device is a chip card.

1 28. A chip card (1) for securely handling an  
2 information unit by interoperating with an  
3 information handling terminal device (2),  
4 comprising a storage (6) for storing an at  
5 least one key for the cryptographic process.

1 29. The chip card according to claim 28, wherein  
2 processing means (7) performing an access  
3 control is controlled by an information unit.

1 30. The chip card according to claim 28, wherein a  
2 processor (7) runs specific functions on the  
3 terminal device (2, 5) or on at least a second  
4 device attached to the terminal device (2, 5).

1 31. The chip card according to claim 28, further  
2 comprising means for transferring of the at  
3 least one second key to the terminal device (2,  
4 5) and/or means for decrypting of the at least  
5 first key by using the at least second key  
6 and/or means to initiate transfer of the  
7 signature key for signature verification.

- 1 32. The chip card according to claim 30, wherein a  
2 non-erasable storage (6) stores the second key  
3 and/or the signature key at time of its  
4 issuing.
- 1 33. The chip card according to claim 32, further  
2 comprising a storage (6) for storing at least a  
3 third key for external authentication and/or  
4 release control of the information unit and  
5 processing means (7) for processing the third  
6 key.
- 1 34. The chip card according to claim 33, wherein  
2 said processing means (7) initiates download of  
3 a new release of the information unit,  
4 depending on the respective status of the third  
5 key.
- 1 35. A chip card accepting device (2), in particular  
2 a chip card reader, for securely handling an  
3 information unit by interoperating with a chip  
4 card (1), comprising a storage for storing the  
5 information unit.
- 1 36. The chip card accepting device according to  
2 claim 35, further comprising means for  
3 decrypting the information unit by using at  
4 least one key.
- 1 37. The chip card accepting device according to  
2 claim 36, further comprising means for  
3 verifying a digital signature.

1 38. The chip card accepting device according to  
2 claim 37, further comprising means for  
3 downloading the encrypted information unit, the  
4 at least one key and the digital signature from  
5 a central server (4).

1 39. The chip card accepting device according to  
2 claim 35, further comprising a storage for  
3 storing at least a third key for external  
4 authentication and/or release control of the  
5 information unit and processing means for  
6 processing the third key.

1 40. The chip card accepting device according to  
2 claim 39, further comprising means to initiate  
3 download of a new release of the information  
4 unit, depending on the respective status of the  
5 third key.

METHOD AND SYSTEM FOR SECURELY HANDLING  
INFORMATION BETWEEN TWO INFORMATION PROCESSING DEVICES

ABSTRACT OF THE DISCLOSURE

Described is a mechanism for securely handling an  
5 information unit by a first information processing device  
(2), for instance a terminal device like a chip card  
reader, which interoperates with a second secure  
information processing device (1), for instance a  
portable device like a chip card, whereby the information  
10 unit is provided by an issuer. The information unit is  
provided from the issuer to the first device and  
encrypted by using a first key. The first key is also  
encrypted by using a second key. The second key is  
provided on the second secure device (1) and  
15 interconnecting the first and the second device enables  
to decrypt the first key by using the second key and then  
to decrypt the information unit by using the first key.

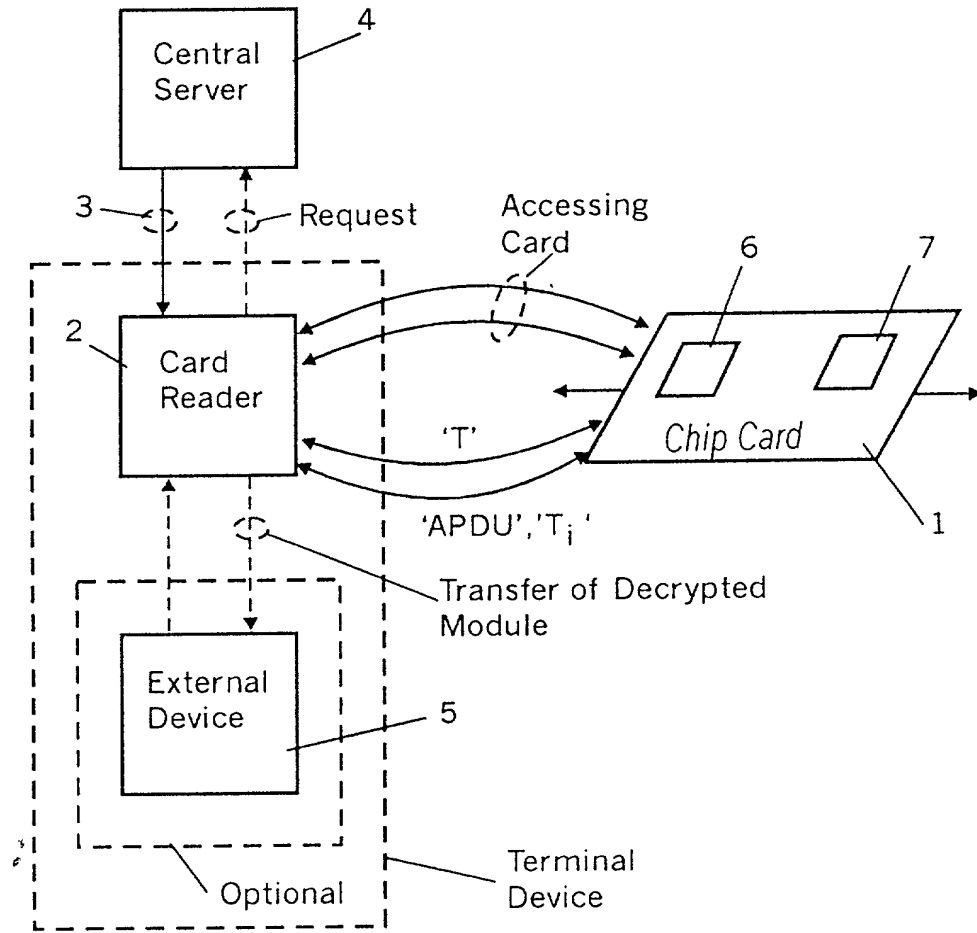


FIG. 1



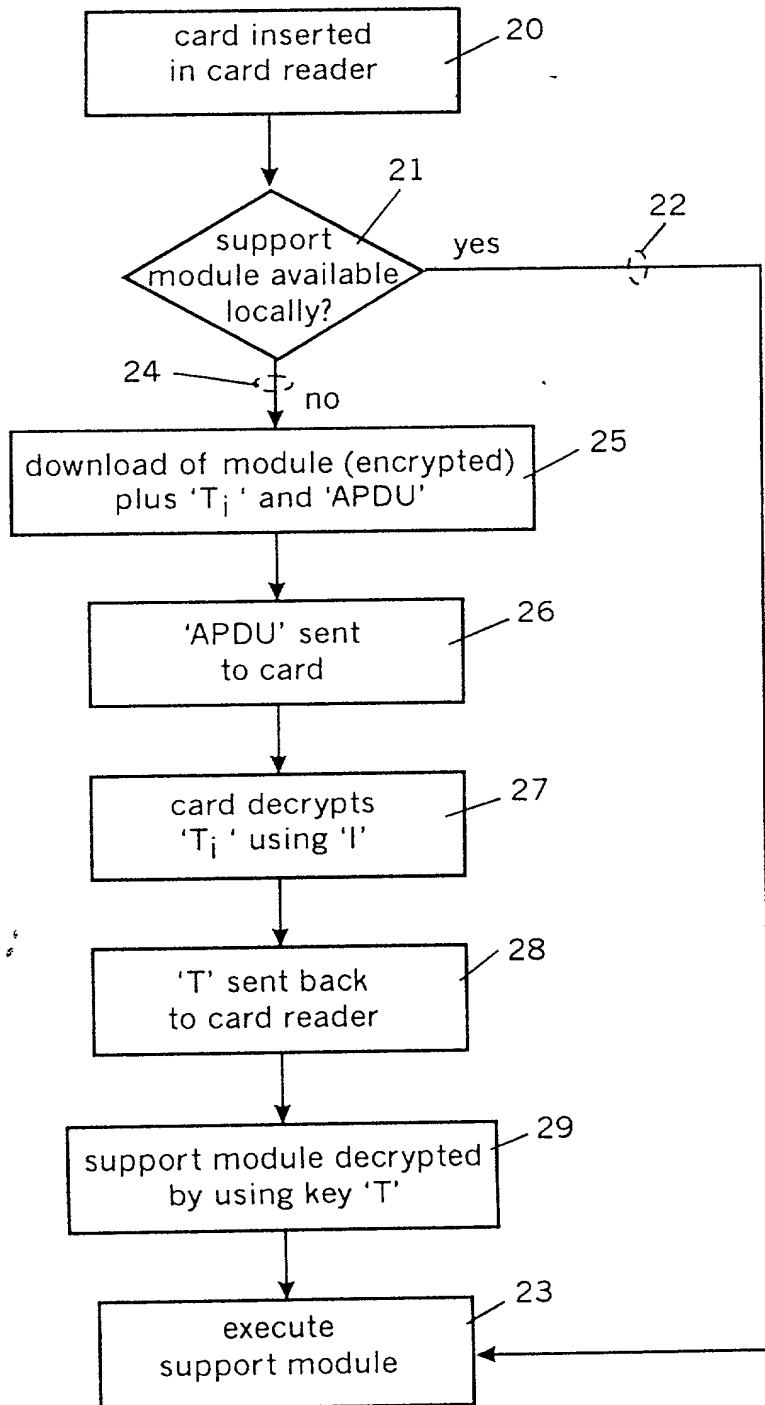


FIG. 2A

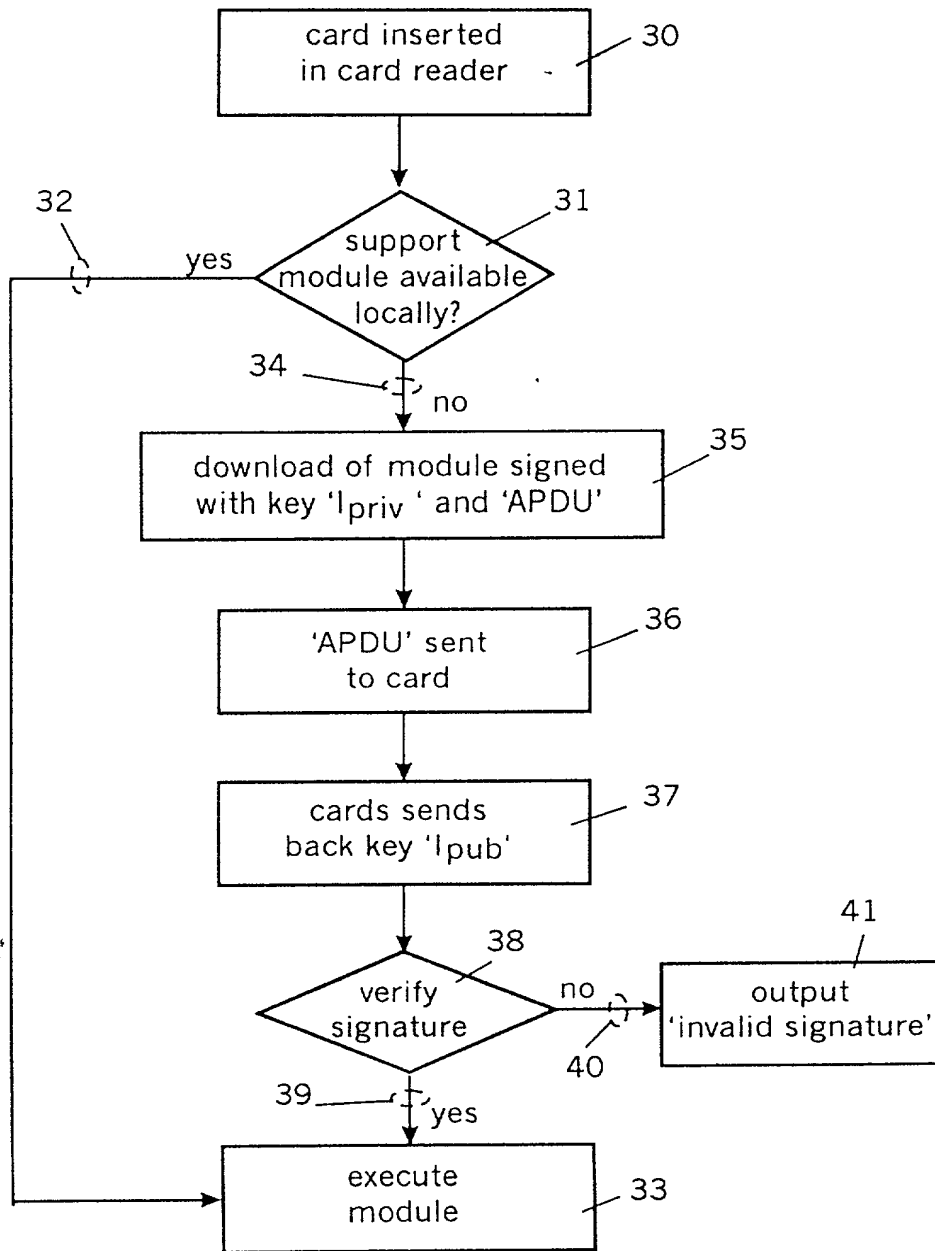


FIG. 2B

# DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD AND SYSTEM FOR SECURELY HANDLING INFORMATION BETWEEN TWO INFORMATION PROCESSING DEVICES  
the specification of which (check one)

X is attached hereto.

\_\_\_\_\_ was filed on \_\_\_\_\_ as United States Application Number \_\_\_\_\_

or PCT International Application Number \_\_\_\_\_

and was amended on \_\_\_\_\_ (if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119(a)-(d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application, having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)		Priority Claimed
99 100 474.8	Europe	12 January 1999
(Number)	(Country)	(Day/Month/Year Filed)
		<u>x</u> Yes ___ No
		___ Yes ___ No
		___ Yes ___ No

I hereby claim the benefit under 35 U.S.C. §119(e) of any United States provisional application(s) listed below.

(Application Number)	(Filing Date)
(Application Number)	(Filing Date)

I hereby claim the benefit under 35 U.S.C. §120 of any United States Application(s), or §365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States, or PCT International application in the manner provided by the first paragraph of 35 U.S.C. §112, I acknowledge the duty to disclose information material to the patentability of this application as defined in 37 CFR §1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith (list name and registration number).

Manny W. Schecter (Reg. 31,722), Terry J. Ilardi (Reg. 29,936), Christopher A. Hughes (Reg. 26,914), Edward A. Pennington (Reg. 32,588), John E. Hoel (Reg. 26,279), Joseph C. Redmond, Jr. (Reg. 18,753), Douglas W. Cameron (Reg. No. 31,596), Kevin M. Jordan (Reg. No. 40,277), Stephen C. Kaufman (Reg. No. 29,551), Daniel P. Morris (Reg. No. 32,053), Louis J. Percello (Reg. No. 33,206), Jay P. Sbrollini (Reg. No. 36,266), David M. Shofi (Reg. No. 39,835), Robert M. Trepp (Reg. No. 25,933) and Louis P. Herzberg (Reg. No. 41,500).

Send Correspondence to: Richard L. Catania, Scully, Scott, Murphy & Presser

400 Garden City Plaza, Garden City, New York 11530

Direct Telephone Calls to: (name and telephone number) Richard L. Catania, (516) 742-4343

Uwe Hansmann

Full name of sole or first inventor

X 

Inventor's Signature

X 14 Sep 1999

Date

Birkenstr. 30/1, D-71155 Altdorf, Federal Republic of Germany

Residence

Germany

Citizenship

Same as above

Post Office Address

Frank Seliger

Full name of second joint inventor, if any

X 

Inventor's signature

X 14 Sep 1999

Date

In den Kriben 25, D-71157 Hildrizhausen, Federal Republic of Germany

Residence

Germany

Citizenship

Same as above

Post Office Address

## PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Uwe Hansmann, et al.      Docket:12640 (GE998-072)

Serial No.: Unassigned      Dated: September 13, 99

Filed: Herewith

For: METHOD AND SYSTEM FOR SECURELY  
HANDLING INFORMATION BETWEEN TWO  
INFORMATION PROCESSING DEVICESAssistant Commissioner for Patents  
Washington, DC 20231ASSOCIATE POWER OF ATTORNEY AND  
REQUEST FOR CHANGE OF MAILING ADDRESS

Sir:

Applicants, by their attorneys of record, hereby grant an  
Associate Power of Attorney to:RICHARD L. CATANIA, Reg. No. 32,608; FRANK S. DIGIGLIO, Reg.  
31,346; KENNETH L. KING, Reg. No. 24,223; STEPHEN D. MURPHY, Reg.  
No. 22,002; LEOPOLD PRESSER, Reg. No. 19,827; JOHN S. SENSNY, Reg.  
No. 28,757; and EDWARD W. GROLZ, Reg. No. 33,705with full power of substitution to prosecute this application and  
transact all business in the United States Patent and Trademark  
Office in connection therewith.Applicants further request that all future correspondence  
in connection with this application be directed and addressed to:RICHARD L. CATANIA, ESQ.  
SCULLY, SCOTT, MURPHY AND PRESSER  
400 Garden City Plaza  
Garden City, New York 11530

Direct all telephone calls to: (516) 742-4343.

Respectfully submitted,

By:

Louis P. Herzberg  
Registration No.: 41,500  
Tel. No.: (914) 945-2885IBM Corporation  
T.J. Watson Research Center  
Route 134/Kitchawan Road  
P.O. Box 218  
Yorktown Heights, New York 10598